MEYER WILSON CO., LPA
Matthew R. Wilson (SBN 290473)
mwilson@meyerwilson.com
Michael J. Boyle, Jr. (SBN 258560)
mboyle@meyerwilson.com
Jared W. Connors (*pro hac vice*)
jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice* to be filed)
sam@turkestrauss.com
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

Attorneys for Plaintiff and the Proposed Class

IN THE DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

SAMANTHA DONELSON, on behalf of herself and all others similarly situated,

Plaintiff,

v.

49ERS ENTERPRISES, LLC d/b/a THE SAN FRANCISCO 49ERS,

Defendant.

Case No. 5:22-cv-05138

Class Action Complaint

Plaintiff Samantha Donelson, through her attorneys, brings this Class Action Complaint against the Defendant, 49ers Enterprises, LLC d/b/a the San Francisco 49ers ("the 49ers" or "Defendant"), alleging as follows:

INTRODUCTION

1. From February 6 to February 11, 2022, the San Francisco 49ers, a National Football League franchise based in the greater San Francisco Bay Area, lost control over at least 20,000 individuals' highly sensitive personal information in a data breach ("Data Breach"), and then failed to notify those individuals about the breach for over six months.

2. Cybercriminals bypassed the 49ers' inadequate security systems using ransomware to

access individuals' personally identifiable information ("PII"), including their names, dates of birth, and Social Security numbers. The cybercriminals also accessed information regarding the employees' immigration statuses and their dependents' PII.

3. From February 6 to February 11, 2022, cybercriminals breached the 49ers' "corporate IT network" and impacted its operations. It is unknown for how long the breach went undetected, meaning the 49ers had no effective means to prevent, detect, or stop the Data Breach from happening before cybercriminals stole and misused PII.

4. Despite public news reports of the incident, it was not until August 9, 2022, that the 49ers' investigation confirmed the unauthorized access to PII stored in its system. Instead of alerting its affected individuals immediately, as required under California law, the 49ers did not disclose the breach until August 31, 2022.

5. On August 31, 2022, the 49ers finally informed affected individuals of the Data Breach and offered them just 12 months of free credit monitoring service, which fails to adequately address the lifelong threat the Data Breach poses to impacted individuals.

6. The 49ers' failures to adequately protect PII stored in its systems and timely notify those affected about the devastating Data Breach harms its current and former employees in violation of California law.

7. Plaintiff Donelson is an employee of another NFL team and a Data Breach victim. She brings this action on behalf of herself and all others harmed by the 49ers' misconduct, seeking relief on a class wide basis.

PARTIES

8. Plaintiff Samantha Donelson, is a natural person and citizen of Georgia, residing in Atlanta, Georgia, where she intends to remain. Plaintiff Donelson received a notice from the 49ers informing her that her personal information was compromised.

9. Defendant 49ers Enterprises, LLC d/b/a the San Francisco 49ers is a Delaware corporation registered to do business in California, with its principal place of business at 4949 Marie P. Debartolo Way, Santa Clara, California 95054.

JURISDICTION & VENUE

10. This Court has jurisdiction over Ms. Donelson's claims under 28 U.S.C. § 1332(d)(2) because there are over 1,000 class members, Ms. Donelson is a citizen of a different state than the 49ers, and the aggregate amount in controversy for the class exceeds $5 million, exclusive of interest and costs.

11. This Court has personal jurisdiction over Defendant because the 49ers are registered to do business in California and is subject to this Court's general and specific jurisdiction given that it is headquartered in California and that this cause of action arises out of events that took place in California.

12. Venue is proper in this District under 28 U.S.C. §§ 1391 because a substantial part of the events or omissions giving rise to the claims emanated from activities within this District and Defendant is headquartered in this District.

BACKGROUND FACTS

a. The 49ers

13. The San Francisco 49ers have been a franchise in the National Football League since 1950, having won five Super Bowl championships in the eighties and early nineties. Since 2014, the 49ers have been based in and around Levi's Stadium in Santa Clara, California.

14. As part of its business operations, the 49ers store PII on its employees, vendors, and other business partners. This information, including names, dates of birth, and Social Security Numbers, was stored on the 49ers internal corporate IT systems.

15. Despite the obvious sensitivity of this information, the 49ers apparently did not implement reasonable cybersecurity safeguards or policies to protect PII, or trained its employees to prevent, detect, and stop data breaches of the 49ers' systems. As a result, the 49ers leave vulnerabilities in its systems for cybercriminals to exploit and give access to PII.

16. In collecting and maintaining the PII, the 49ers implicitly agree it will safeguard the data using reasonable means according to its internal policies and state and federal law.

17. Despite its duties to safeguard PII, on February 6, 2022, cybercriminals bypassed the 49ers' security systems undetected and accessed PII as part of a "ransomware" attack.

18. As of at least February 13, 2022,[1] there were public reports that the 49ers were subject to a ransomware attack. Despite these reports, the 49ers did not immediately inform affected or potentially affected individuals about the breach or otherwise notify them according to California law. Instead, the 49ers initiated an internal investigation to "identify the individuals whose information was contained in the files."[2] This investigation, according to the 49ers, took until August 9, 2022. During the investigation, the 49ers did not contact any of the affected individuals.

19. On information and belief, the currently unidentified cybercriminals utilized a type of ransomware called "BlackByte" to penetrate the 49ers' systems. In fact, BlackByte listed the 49ers on its website as a system successfully penetrated by the program.[3]

20. On August 31, 2022, the 49ers finally notified affected individuals of the Data Breach ("Breach Notice")— nearly six months after the Data Breach.[4]

21. Despite "investigating" the Data Breach for several months, the 49ers' Breach Notice revealed little about the breach and obfuscated its nature. The 49ers' Breach Notice assures affected individuals that "We take this situation seriously," telling them that the 49ers is "taking steps to prevent something like this from occurring again, including additional measures to further enhance our security protocols and continued education and training to our employees"—steps that should have taken place *before* the Data Breach.

22. The 49ers' Breach Notice informs Data Breach victims they can sign up for 12 months of free credit monitoring, which does not adequately address the lifelong harm that the Data Breach poses to its victims.

---

[1] https://www.cnn.com/2022/02/13/us/49ers-network-security-incident/index.html (last accessed September 8, 2022).

[2] https://oag.ca.gov/system/files/SF%2049ers%20-%20California%20Notification.pdf (last accessed September 8, 2022).

[3] *See* https://www.cnn.com/2022/02/13/us/49ers-network-security-incident/index.html (last accessed September 8, 2022).

[4] A true and accurate copy of the Breach Notice is attached as **Exhibit A.**

23. The 49ers' Breach Notice does not explain how the hack happened, why it took so long for the 49ers to discover it, what exactly cybercriminals stole, and why it took the 49ers nearly 6 months to disclose the breach in a bare-bones notice.

24. On information and belief, the 49ers failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over PII it stored in its systems. The 49ers' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII.

25. By obtaining, collecting, and storing the PII of Plaintiff Donelson and the Class, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

26. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and the Class.

c. Plaintiff's Experience

27. Plaintiff Donelson is an employee of the Atlanta Falcons, another franchise in the NFL.

28. Ms. Donelson works for the Falcons in their live events department. As part of her work for the Falcons, Ms. Donelson provided her information to the 49ers.

29. Plaintiff Donelson provided her PII to the 49ers and trusted that the company would use reasonable measures to protect it according to the 49ers internal policies, as well as state and federal law.

30. As a result of a previous data breach, Plaintiff Donelson utilized Credit Wise, a credit monitoring service provided via Capital One.

31. In February 2022—soon after the 49ers breach—Credit Wise informed Plaintiff Donelson that her Social Security number had been used on the "dark web." On information and belief, the "dark web" is an internet portal where compromised identities can be traded or sold by cybercriminals.

32. At the time, Plaintiff Donelson had no way to connect this incident to the 49ers Data Breach, and no substantive information regarding who was affected was available.

33. Plaintiff Donelson has and will spend considerable time and effort monitoring her

accounts to protect herself from identity theft.

34. On September 5, 2022, Plaintiff Donelson received notice from the 49ers that her name, date of birth, and Social Security Number was compromised as part of the Data Breach.

35. Plaintiff Donelson suffered actual injury and damages due to Defendant's failure to secure and safeguard her PII before the Data Breach.

36. Plaintiff Donelson suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant as part of her job duties in the NFL organization.

37. Plaintiff Donelson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

38. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

39. Plaintiff Donelson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

40. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

41. As a result of the 49ers' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered, or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

42. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

43. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

44. It can take victims years to stop identity or PII theft, giving criminals plenty of time to use that information for cash.

45. One such example of criminals using PII for profit is the development of "Fullz" packages.

46. Cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

47. The development of "Fullz" packages means that stolen PII from the Data Breach can

easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

48. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

49. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. **Defendant Violated the FTC Act**

50. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

51. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

52. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

53. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

54. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

57. Under Fed.R.Civ.P. 23, Plaintiff sues on behalf of herself and the proposed Class ("Class"), defined as follows:

All individuals whose PII was compromised in the Data Breach disclosed

by the San Francisco 49ers on or about August 31, 2022. T

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

58. Plaintiff reserves the right to amend the class definition.

59. *Ascertainability.* The 49ers have identified, or are able to identify, all individuals affected by the data breach. These records will identify the Class Members.

60. *Numerosity.* The class includes approximately 20,000 class members, so individual joinder would be impracticable.

61. *Commonality and Predominance.* This case presents questions of law and fact common to all class members, and those common questions predominate over individualized issues. These common questions include:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contractual promises to safeguard Plaintiff and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

b. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

c. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

d. **Superiority.** Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individuals are insufficient to make individual lawsuits economically feasible.

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

62. Plaintiff realleges all previous paragraphs as if fully set forth below.

63. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

64. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

65. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

66. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII.

67. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

68. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

69. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

70. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

71. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary

damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

72. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II

Negligence Per Se

(On Behalf of Plaintiff and the Class)

73. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

74. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

75. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

76. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

77. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

78. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

79. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

80. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

81. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

82. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

83. Had Plaintiff and members of the Class known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

84. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III

Breach of an Implied Contract

(On Behalf of Plaintiff and the Class)

85. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

86. Defendant offered to employ Plaintiff and members of the Class in exchange for their PII.

87. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employee PII.

88. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

89. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

90. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

91. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

92. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

93. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

94. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

95. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

96. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

97. In these and other ways, Defendant violated its duty of good faith and fair dealing.

98. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV

Unjust Enrichment

(On Behalf of Plaintiff and the Class)

99. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

100. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

101. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to facilitate their employment.

102. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

103. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendant

failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

104. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT V

Violation of California's Consumer Records Act

Cal. Civ. Code § 1798.80, *et seq.*

(On behalf of Plaintiff and the Class)

105. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

106. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (*Id.*), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

107. The Data Breach constitutes a "breach of the security system" of Defendant.

108. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

109. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class, but waited approximately three months to notify them. Three months is an unreasonable delay under the circumstances.

110. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

111. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

112. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT VI

Violation of California's Unfair Competition Law

Cal. Bus. Code § 17200, *et seq.*

(On behalf of Plaintiff and the Class)

113. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

114. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

115. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

116. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure so as to prevent the loss or misuse of that PII.

117. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

118. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

119. Had Defendant complied with these requirements, Plaintiff and the Class would not

have suffered the damages related to the data breach.

120. Defendant's conduct was unlawful, in that it violated the CCPA.

121. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

122. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

123. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

124. Instead, Defendant made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

125. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

126. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

127. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

128. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VII

Violation of the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150

(On behalf of Plaintiff and the Proposed Class)

129. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

130. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the Class. As a direct and proximate result, Plaintiff's, and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

131. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its employees and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

132. Plaintiff and class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's and Class members' PII. Plaintiff and Class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

133. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff

intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

134. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

135. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED on September 9, 2022.

By: */s/ Michael J. Boyle, Jr.*
Matthew R. Wilson (Bar No. 290473)
Email: mwilson@meyerwilson.com
Michael J. Boyle, Jr. (Bar No. 258560)
Email: mboyle@meyerwilson.com
Jared W. Connors (*Subject to Pro Hac Vice Admission*)
Email: jconnors@meyerwilson.cm
MEYER WILSON CO., LPA
305 W. Nationwide Blvd.
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

Samuel J. Strauss
(*Subject to Pro Hac Vice Admission*)
Raina Borrelli
(*Subject to Pro Hac Vice Admission*)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Tel: 608-237-1775
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and the Proposed Class